

Network Services in Virtualized Data Center

Tomáš Michaeli

Consulting Systems Engineer, DCV Central / Czech republic

21 Mar 2012

DC Market

- Almost 60% of all datacenter workloads are virtualized
- Computing model has changed
- IT Service model has changed

Cisco

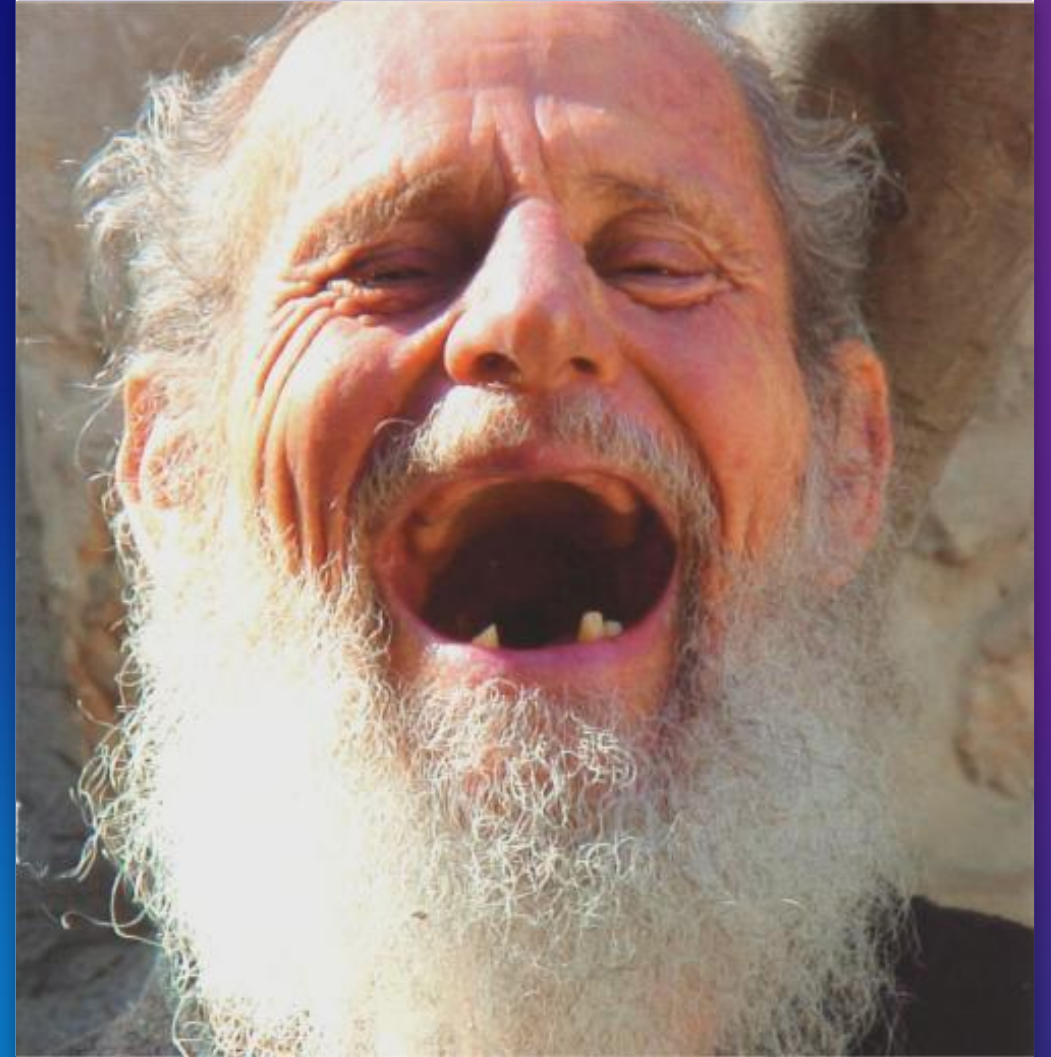
- Company extending direction for some products from purely HW based appliance to SW based virtual service node
- Easy service integration in virtual environment
- Cloud based automation
- Physical -> Virtual -> Cloud Journey

VMware, Microsoft, Citrix, RedHat, Oracle

- VMware gain significant share on hypervisor market
- Windows 8 behind the corner
- Hypervisor market transforms to cloud market
- Competitors in one space, friends in other

**Data Center, Services, &
Virtualization: It's so
easy!**

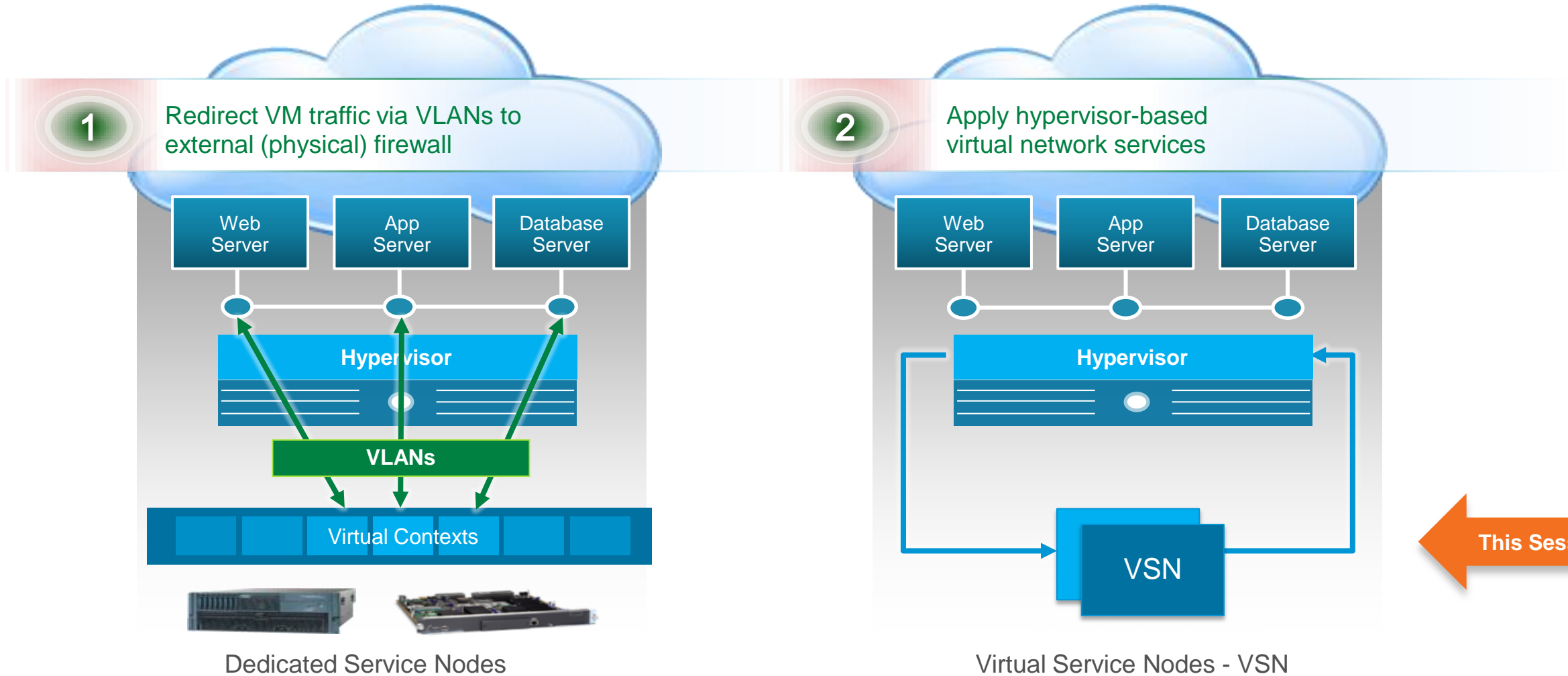
**Just ask this 35 year old
Administrator.**



Agenda

- Architecture for virtualized services
- Understanding vPath and VXLAN
- Virtual Security Gateway with vPath Integration
- Nexus 1000V with VXLAN Integration with VMware vCloud Director
- Virtual ASA role in overall architecture
- Virtual WAAS integration
- Summary
- Resources

Network Services Options for Virtualized/Cloud DC



Virtual Services Node Options

- Stand-alone VSN

Can be deployed with any virtual switch

Example: vWAAS

- N1KV vPath integrated VSN

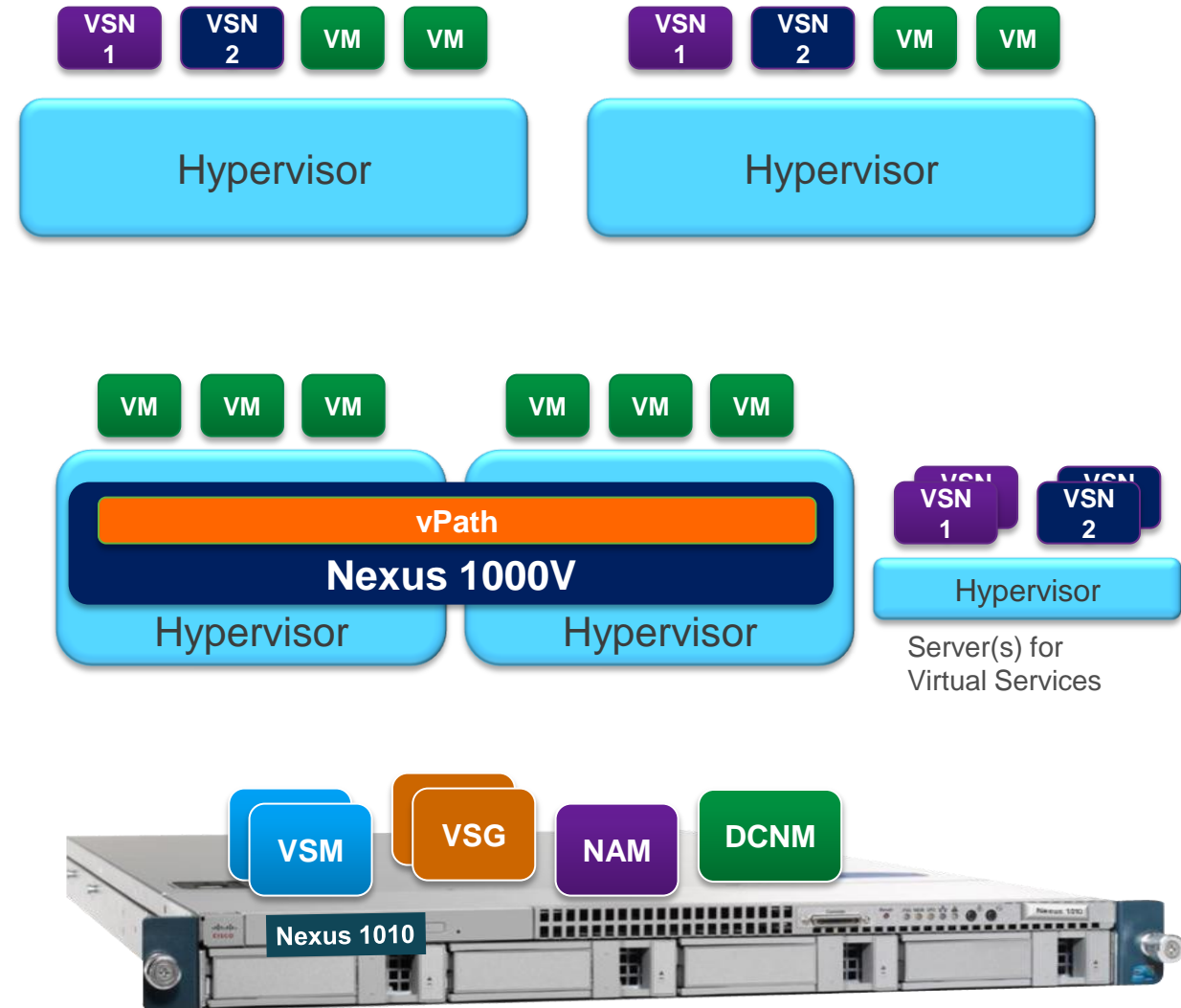
Integrates with N1KV port profile and virtual service datapath (vPath)

Example: vWAAS, VSG, ASA 1000V

- VSN hosted on Nexus 1010 appliance

VSN can be stand-alone or vPath integrated

Example: VSG, NAM



Virtual Services – Architectural Approach

Requirement	Solution
Virtualization Awareness <ul style="list-style-type: none">• Dynamic policy-based provisioning• Support VM mobility (e.g. vMotion)	<ul style="list-style-type: none">• Virtual (SW) form-factor• Integration with VM mgmt tools (e.g. vCenter, SC-VMM in future)• Policies bound to vNIC/VM<ul style="list-style-type: none">• Integration with N1KV (vPath*)
Multi-tenant / Scale-out deployment	<ul style="list-style-type: none">• Virtual service: multi-instance deployment• Management: Multi-tenant• N1KV vPath: Multi-tenant
Separation of Duties <ul style="list-style-type: none">• Non-disruptive to server team	<ul style="list-style-type: none">• Profile-based provisioning for services• Integration with N1KV port profile• Optional hosting on Nexus 1010 HW appliance
<ul style="list-style-type: none">• Efficient deployment• Performance optimization	Integration with N1KV vPath
Extended mobility <ul style="list-style-type: none">• DC-wide, DC-to-DC, DC-to-Cloud	<ul style="list-style-type: none">• DC-wide: VXLAN• DC-to-DC: OTV, FabricPath

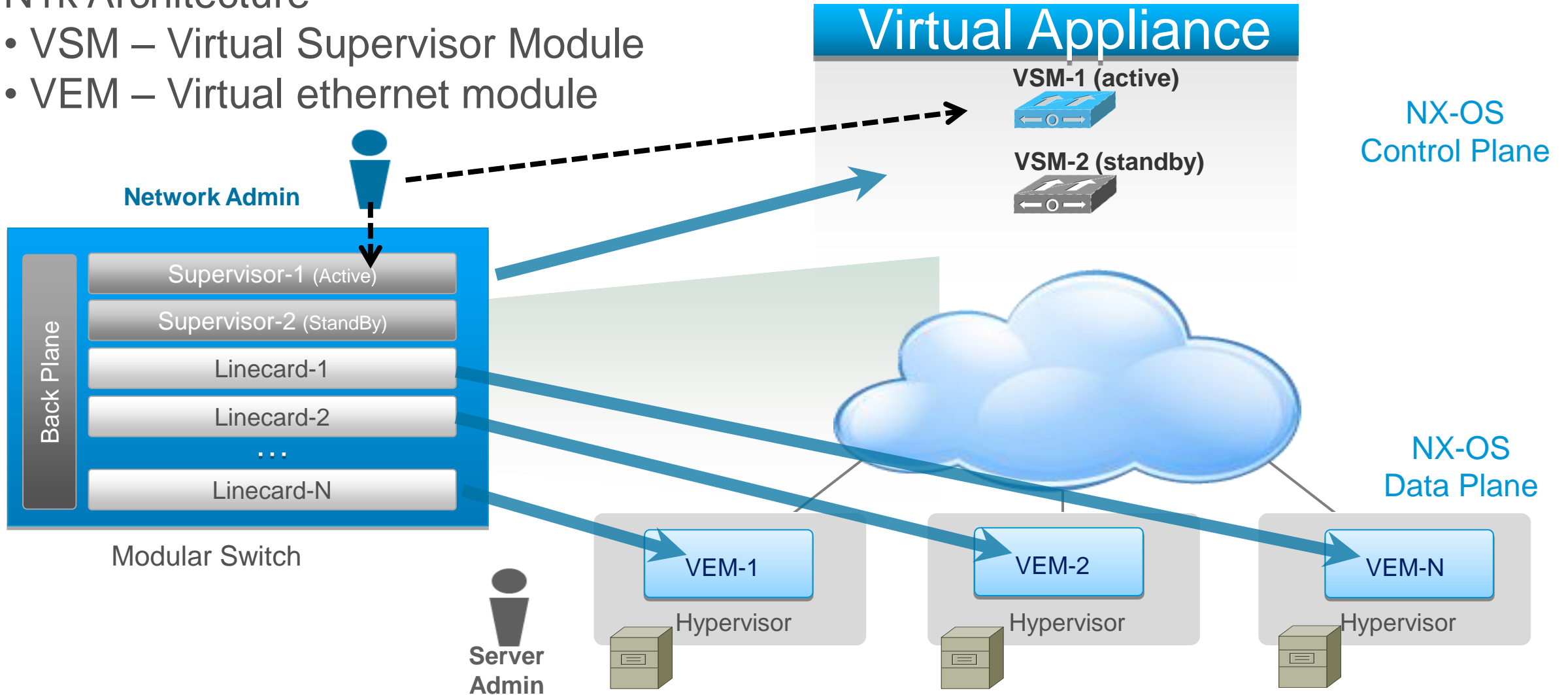
Architecture for virtualized services



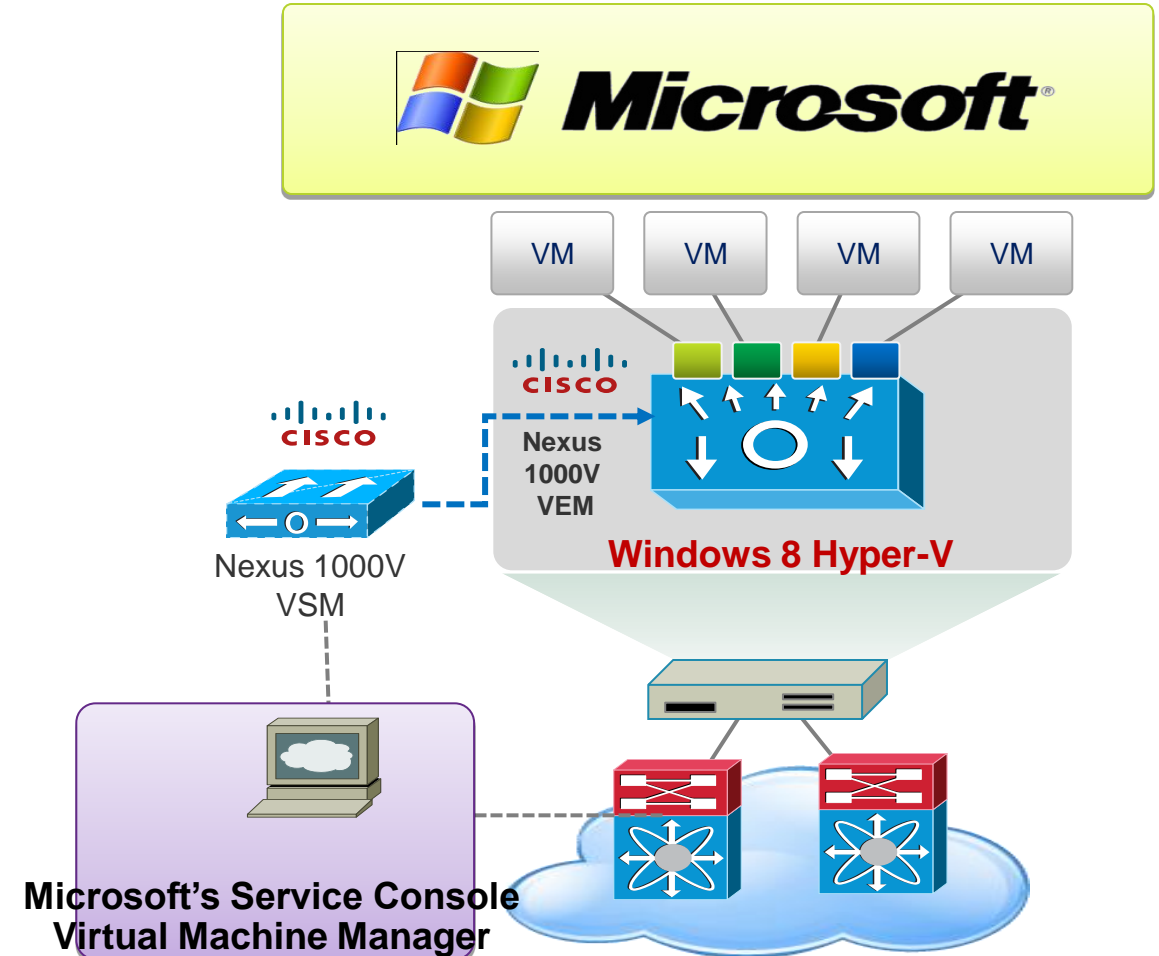
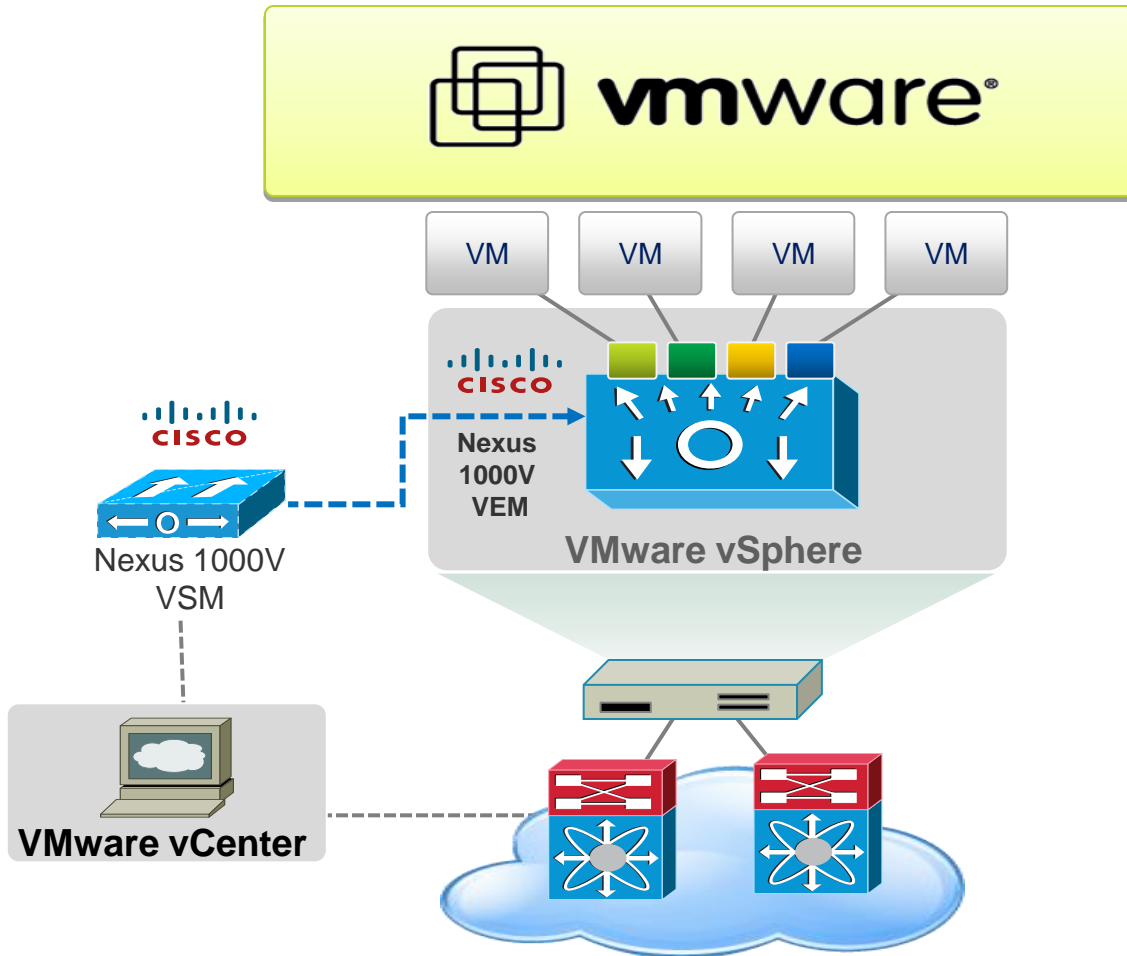
Network team manages virtual & physical networks

N1k Architecture

- VSM – Virtual Supervisor Module
- VEM – Virtual ethernet module



Consistent across Hypervisors



Virtual Services Portfolio

Virtual Appliance

Virtual ASA



vWAAS



VSG



ACE



VSM: Virtual Supervisor Module

VSG: Virtual Security Gateway

ACE: Virtual Load Balancer

vWAAS: Virtual WAAS

Virtual ASA: Tenant-edge security

Nexus 1010 / 1010X

Primary



Secondary



Virtual Blades

Virtual Supervisor Module (VSM)

Network Analysis Module (NAM)

Virtual Security Gateway (VSG)

Data Center Network Manager (DCNM)

L3 Connectivity

vPath

- Virtual service data-path

VEM-1

vPath

VXLAN

VMware ESX



VEM-2

vPath

VXLAN

VMware ESX



VEM-1

vPath

VXLAN

Win 8 Hyper-V



VEM-2

vPath

VXLAN

Win 8 Hyper-V

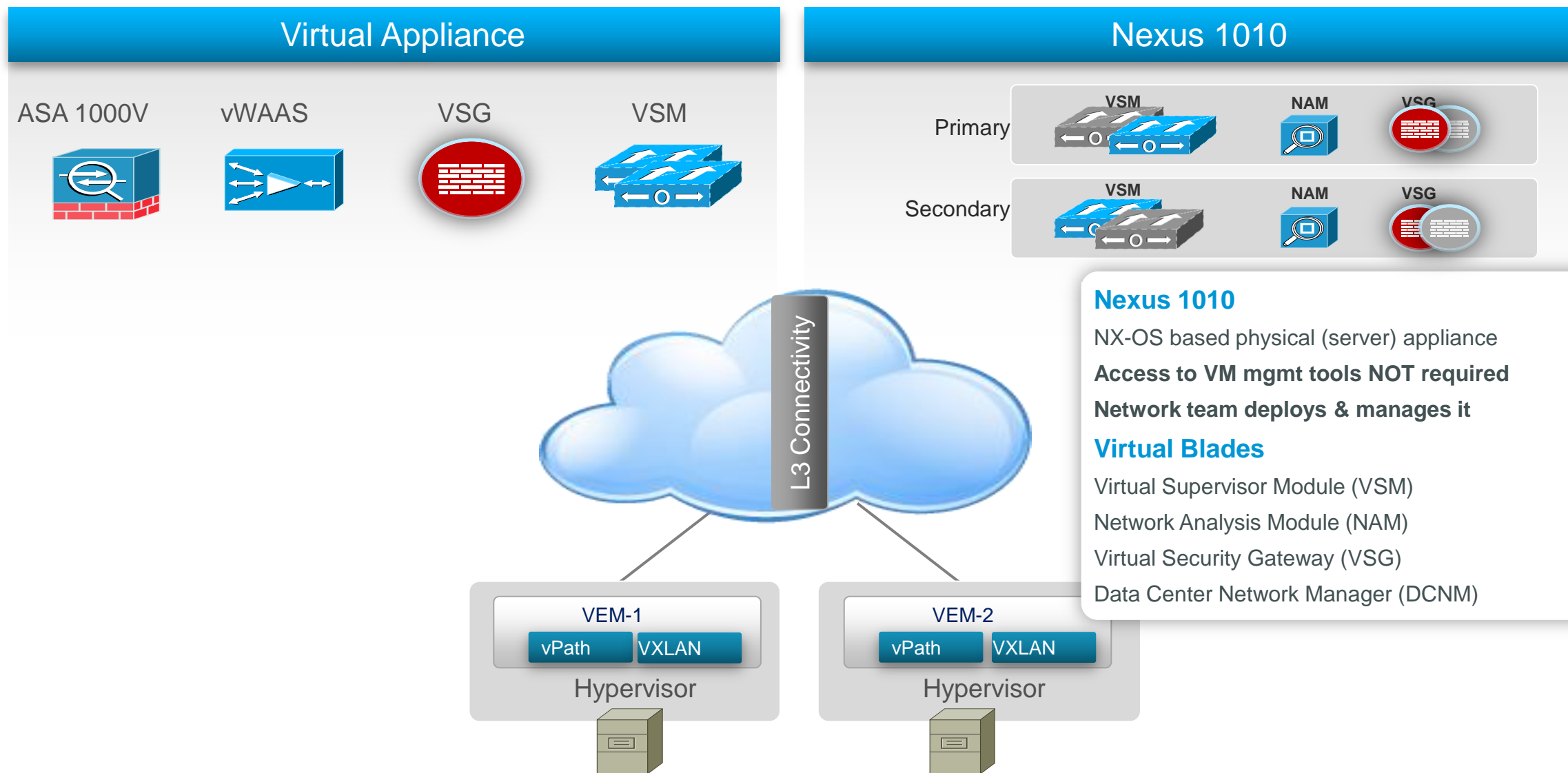


VXLAN

- Scalable Segmentation

Nexus 1010

Hosting Platform for Virtual Services



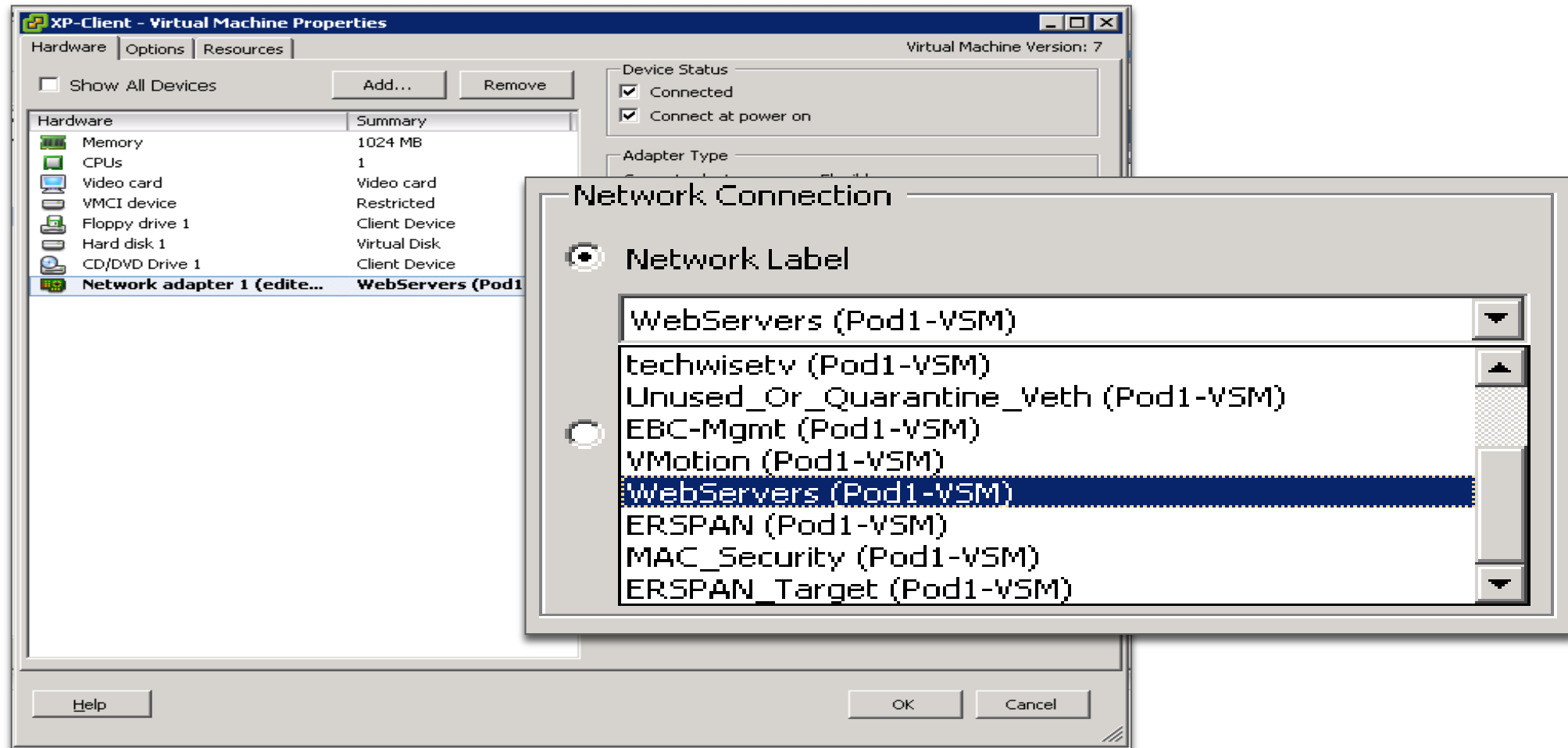
Network Guy - Port Profile Configuration

```
n1000v# show port-profile name WebServers
port-profile WebServers
  description:
  status: enabled
  capability uplink: no
  system vlans:
  port-group: WebServers
  config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 110
    no shutdown
  assigned interfaces:
    Veth10
```

Support Commands Include:

- ✓ Port management
- ✓ VLAN
- ✓ PVLAN
- ✓ Port-Channel
- ✓ ACL
- ✓ Netflow
- ✓ Port security
- ✓ QoS

Server Guy – Server configuration



Network guy - Troubleshooting

Port Profile

mgmt

uplink

Win2k8_AD

Nexus1000V#
session 1

description

type

state

source intf

rx

tx

both

source VLANs

rx

tx

both

filter VLANs

destination

ERSPAN ID

ERSPAN TTL

ERSPAN IP Pr

ERSPAN DSCP

Windows 7 - VMware Workstation

File View VM

Capturing from Intel(R) PRO/1000 MT Network Connection - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: `erspan.spanid == 999 && (icmp.type == 8 || icmp.type == 0)` Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
458	104.998509	192.168.1.11	192.168.1.1	ICMP	Echo (ping)
459	104.998571	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
460	104.998779	192.168.1.1	192.168.1.11	ICMP	Echo (ping)
461	104.998801	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
462	105.998393	192.168.1.11	192.168.1.1	ICMP	Echo (ping)
463	105.998454	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
464	105.998890	192.168.1.1	192.168.1.11	ICMP	Echo (ping)
465	105.998912	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
466	106.998640	192.168.1.11	192.168.1.1	ICMP	Echo (ping)
467	106.998696	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
468	106.998900	192.168.1.1	192.168.1.11	ICMP	Echo (ping)
469	106.998922	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
470	107.998467	192.168.1.11	192.168.1.1	ICMP	Echo (ping)
471	107.998528	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
472	107.998797	192.168.1.1	192.168.1.11	ICMP	Echo (ping)
473	107.998818	192.168.1.12	192.168.1.102	ICMP	Destination Unreachable
474	108.998564	192.168.1.11	192.168.1.1	ICMP	Echo (ping)

Frame 6 (124 bytes on wire, 124 bytes captured)

Ethernet II, Src: Vmware_72:03:4a (00:50:56:72:03:4a), Dst: Vmware_89:00:06 (00:50:56:89:00:06)

Internet Protocol Src: 192.168.1.102 (192.168.1.102), Dst: 192.168.1.12 (192.168.1.12)

0000 00 50 56 89 00 06 00 50 56 72 03 4a 08 00 45 00 .PV...P Vm...E.
0010 00 6e 36 cd 00 00 40 2f bf d1 c0 a8 01 66 c0 a8 .n6...@/f..
0020 01 0c 10 00 88 be 00 00 00 00 10 0b 03 e7 9c 00
0030 00 20 00 50 56 89 00 00 00 50 56 89 00 01 08 00 . .PV... .PV.....
0040 45 00 00 3c 02 d5 00 00 80 01 b4 8f c0 a8 01 0b E...<.....
0050 c0 28 01 01 08 00 4c 74 00 01 00 07 61 62 63 64

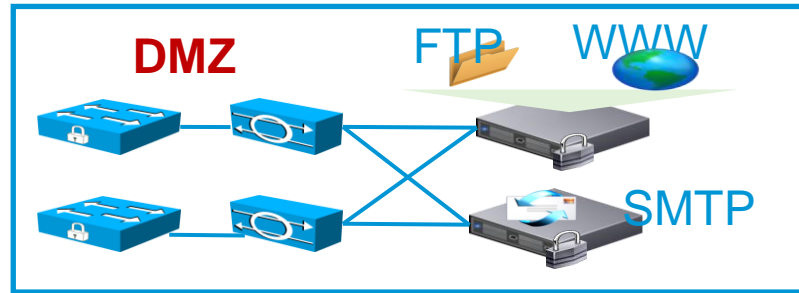
Intel(R) PRO/1000 MT Network Connection: ... Packets: 474 Displayed: 437 Marked: 0 Profile: Default

4:14 AM 8/14/2010

Why N1kV ?

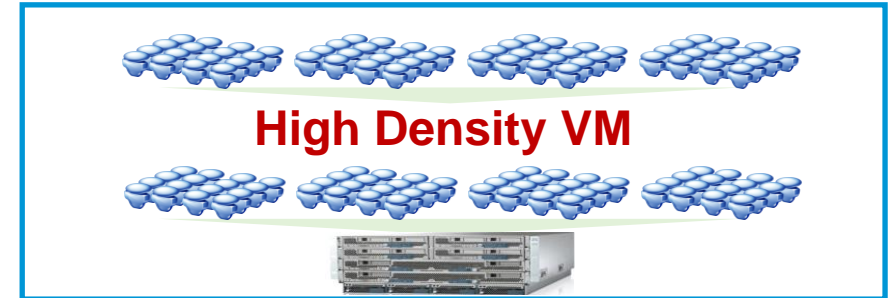
Use Cases

- Visibility & Monitoring
- Secure multi-tenancy
- DMZ Virtualization
- Virtual Desktops
- Compliance
- Cloud Infrastructures
- Separation of duties



Architectural Benefits

- End-to-end Nexus consistency
- Advanced NX-OS features
- Virtual Services & vPath
- Reference Architectures



Nexus 1000V Interoperability with VMware

VMware Product	Nexus 1000V support
vSphere 4	✓
vSphere 5 (with stateless ESX)	✓ (Release 1.4a & above)
VMware View 5	✓
VMware vCloud Director • Port-group backed pools	✓
VMware vCloud Director 1.5 • Port-group backed pools • VLAN-backed pools • Network-isolation backed pools (via VXLAN)	✓ (vCD 1.5 Update release)

Understanding vPath and VXLAN



Virtualized Network Services – vPath

vPath is a part of N1kV

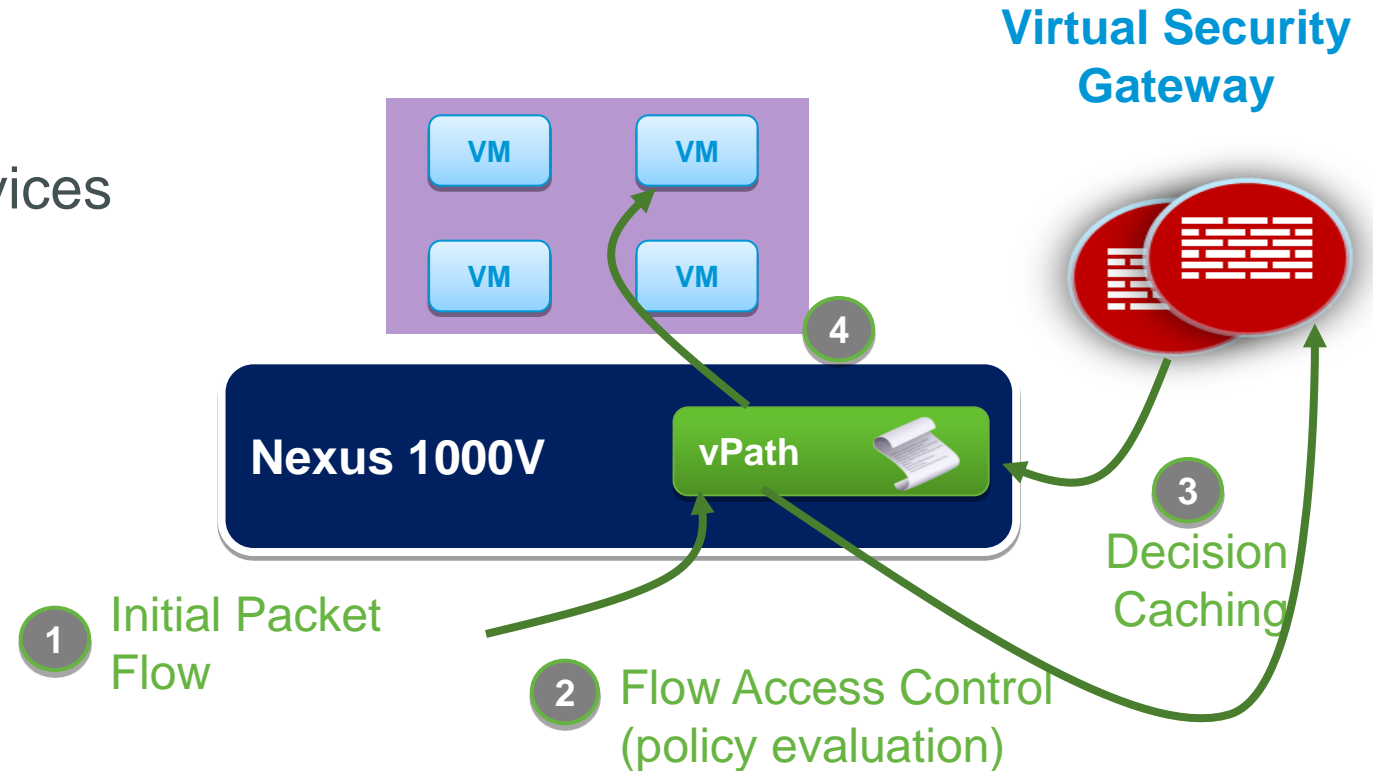
vPath 1.5 available

- Designed for virtualized network services
- VEM to VSN supporting L3
- Service Binding (Traffic Steering)

- Fast-Path Offload

vPath 2.0 (Q2CY12)

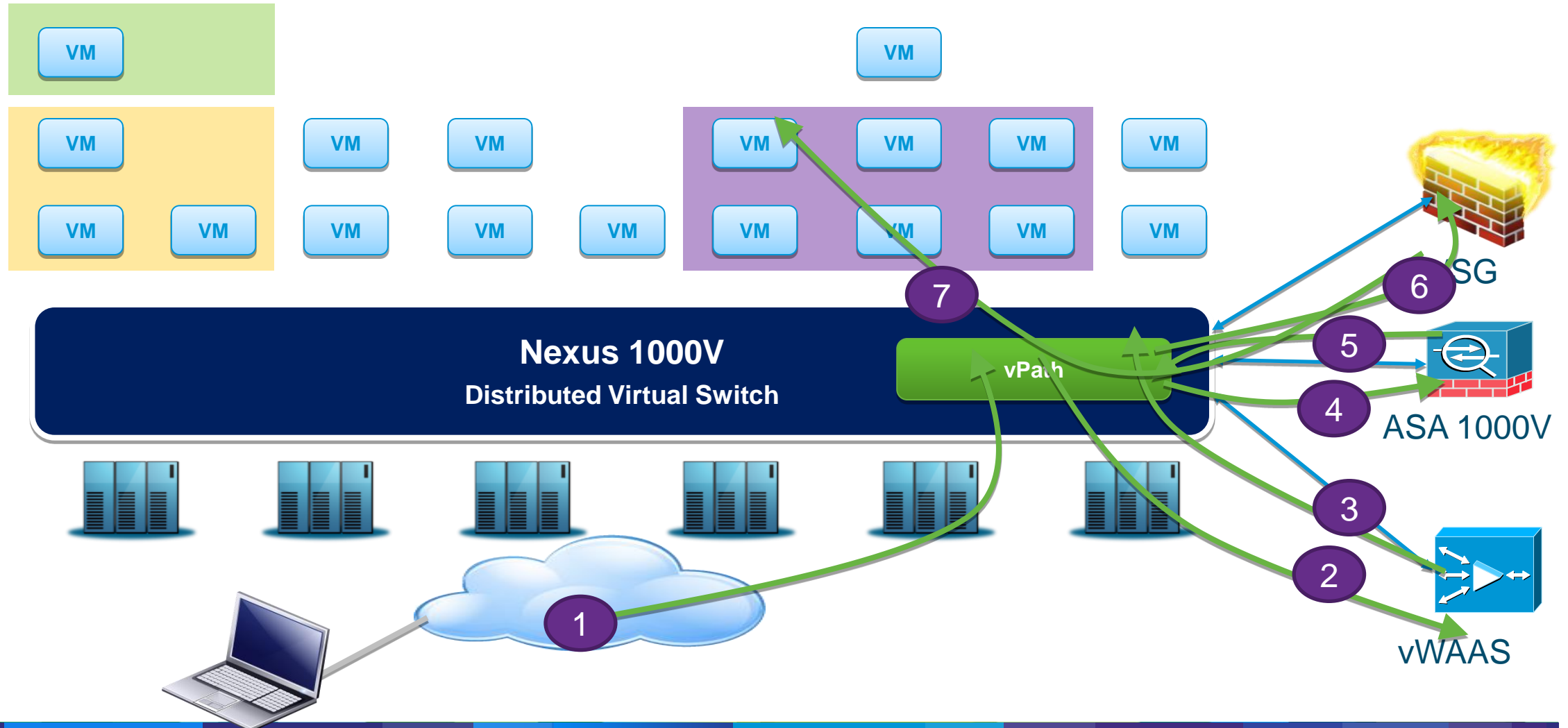
- VSN on VXLAN
- Service chaining



L3 vPath Requirements

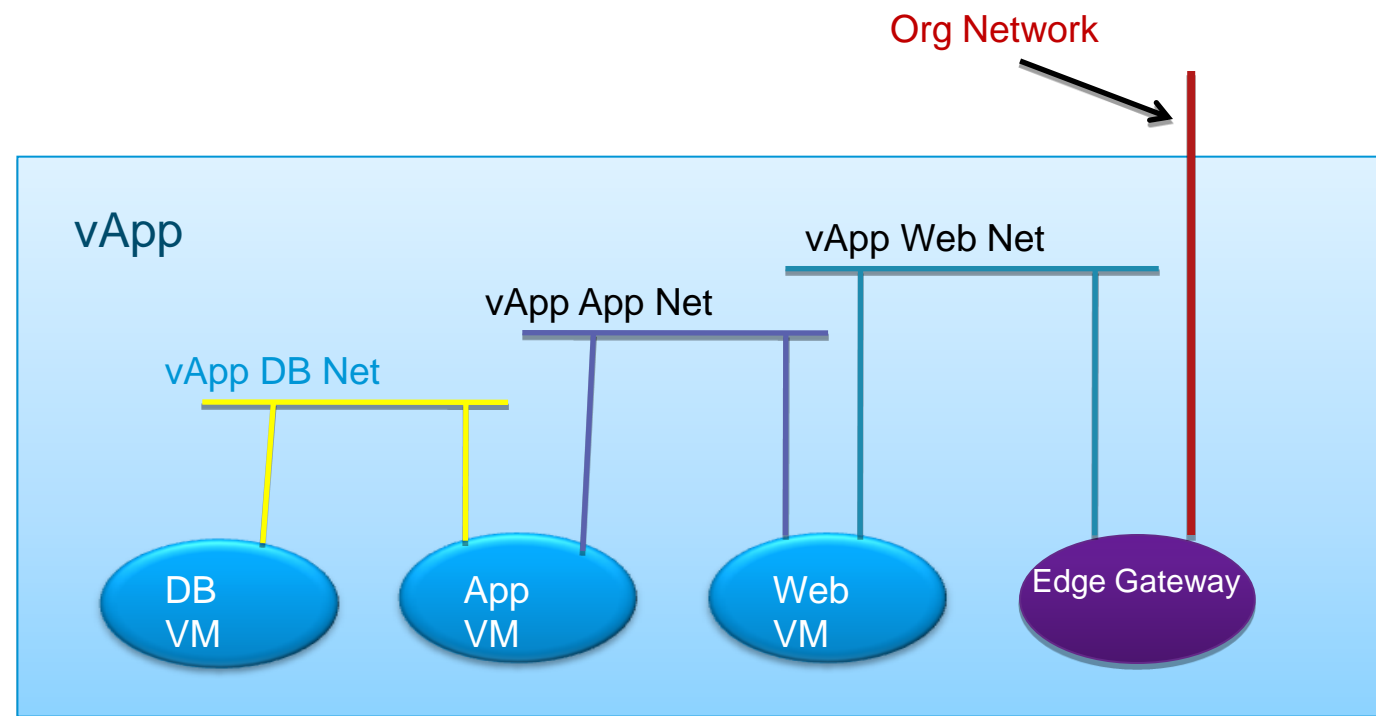
- For routing proxy ARP must be enabled on first hop router
- All vmknics must be able to reach the L3 VSG.
- Fragmentation is not supported
- Uplink MTU +96B

vPath 2.0 – Service Chaining



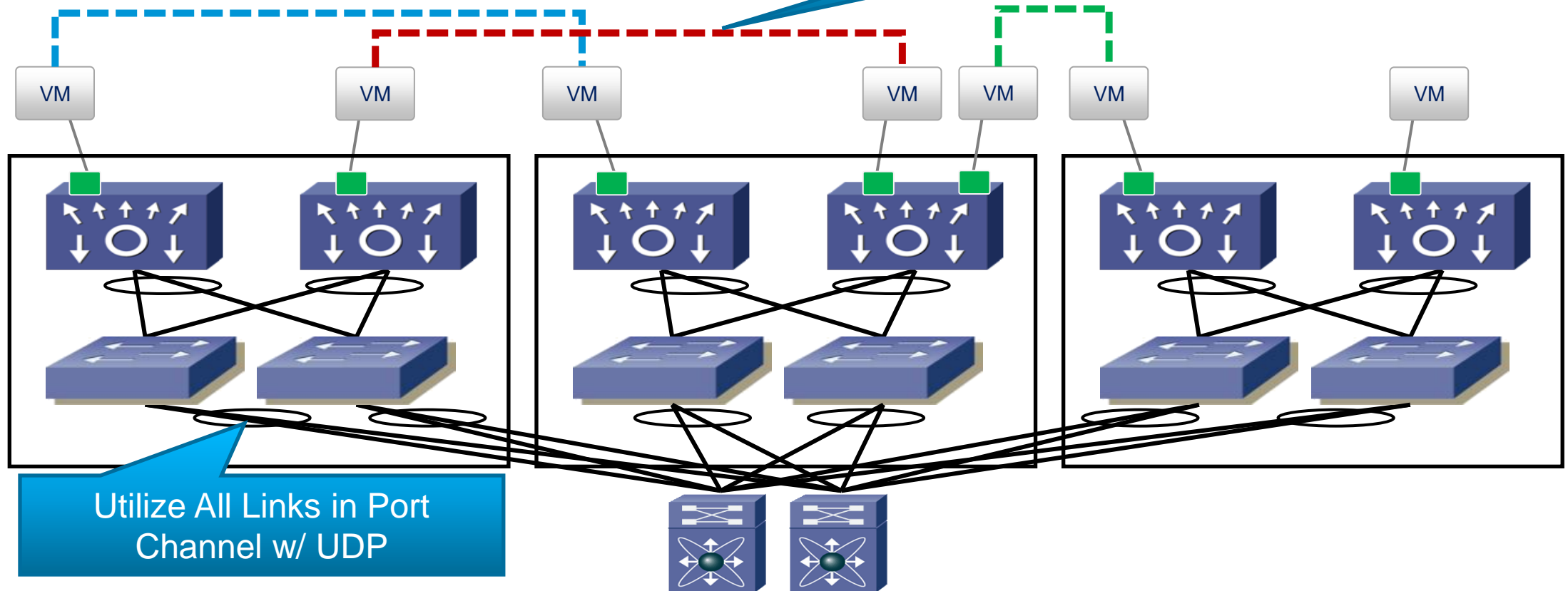
vCloud Director – vApp problem

- vCD Providers offer catalogs of vApps
- Clone new vApp = same MAC and IP addresses
- L2 isolation is required
- Usage of vApps causes an explosion in the need for isolated L2 segments
- vApps NEEDS MORE VLANS !!!
- VXLAN 16k ID's



Cloud on physical DC / Scalability – VXLAN

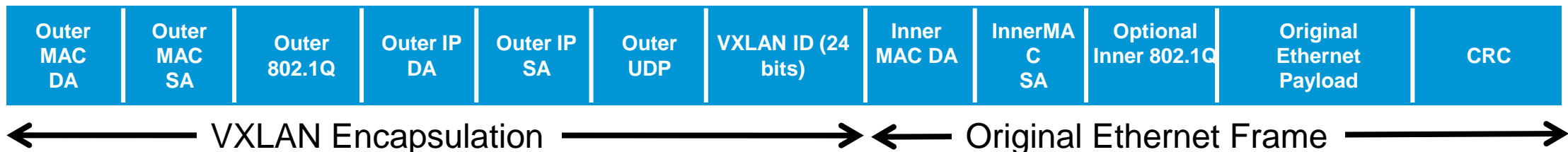
Logical Network Spanning Across Layer 3



Add More Pods to Scale

Virtual Extensible Local Area Network – VXLAN

- Ethernet in IP overlay network
 - Entire L2 frame encapsulated in UDP
 - 50 bytes of overhead
- Include 24 bit VXLAN Identifier
 - 16 M logical networks
 - Mapped into local bridge domains
- VXLAN can cross Layer 3
- Tunnel between VEMs
 - VMs do NOT see VXLAN ID
- IP multicast used for L2 broadcast/multicast, unknown unicast
- Technology submitted to IETF for standardization
 - With VMware, Citrix, Red Hat, Broadcom, Arista, and Others



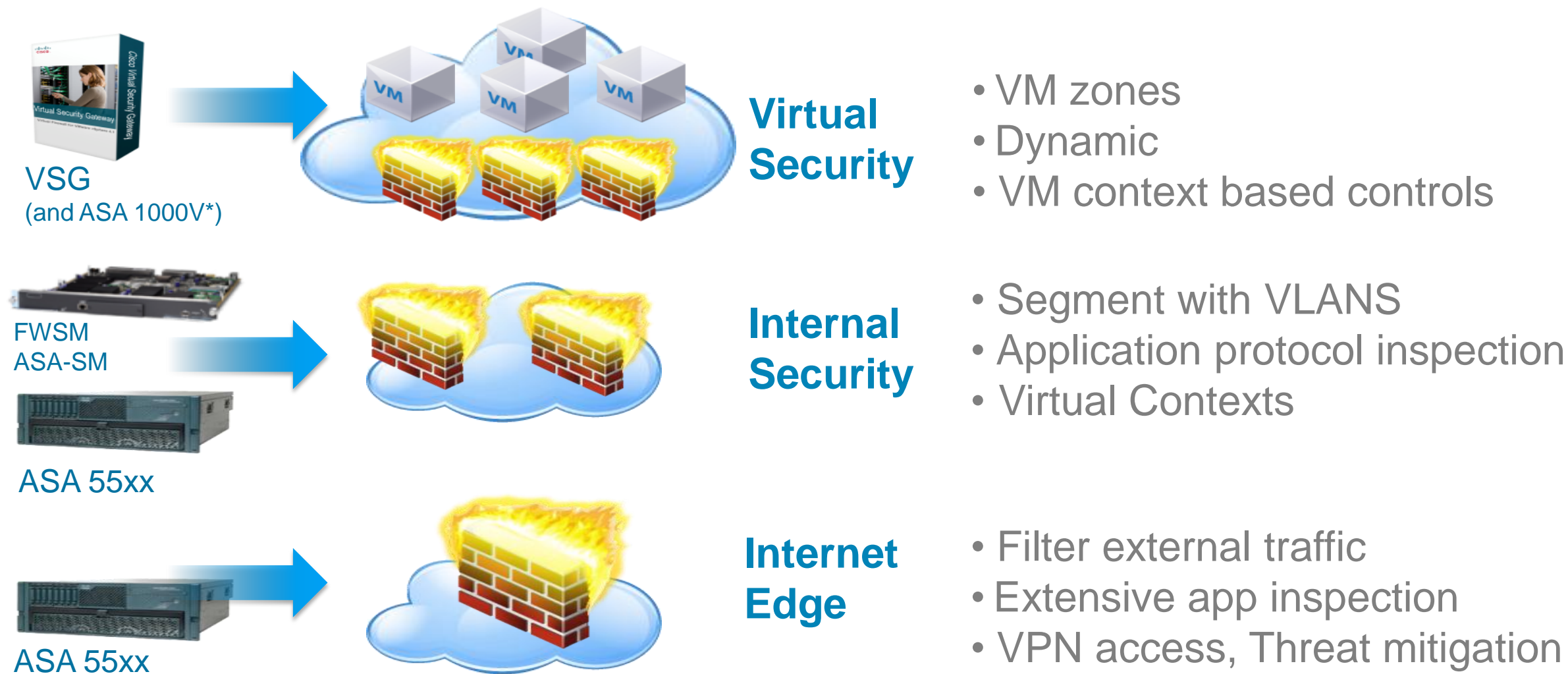
VXLAN Infrastructure Prerequisites

- For routing proxy ARP must be enabled on first hop router
- IP Multicast forwarding is required
- Increased MTU needed +50B
- Leverage 5-tuple hash distribution for uplink and interswitch LACP

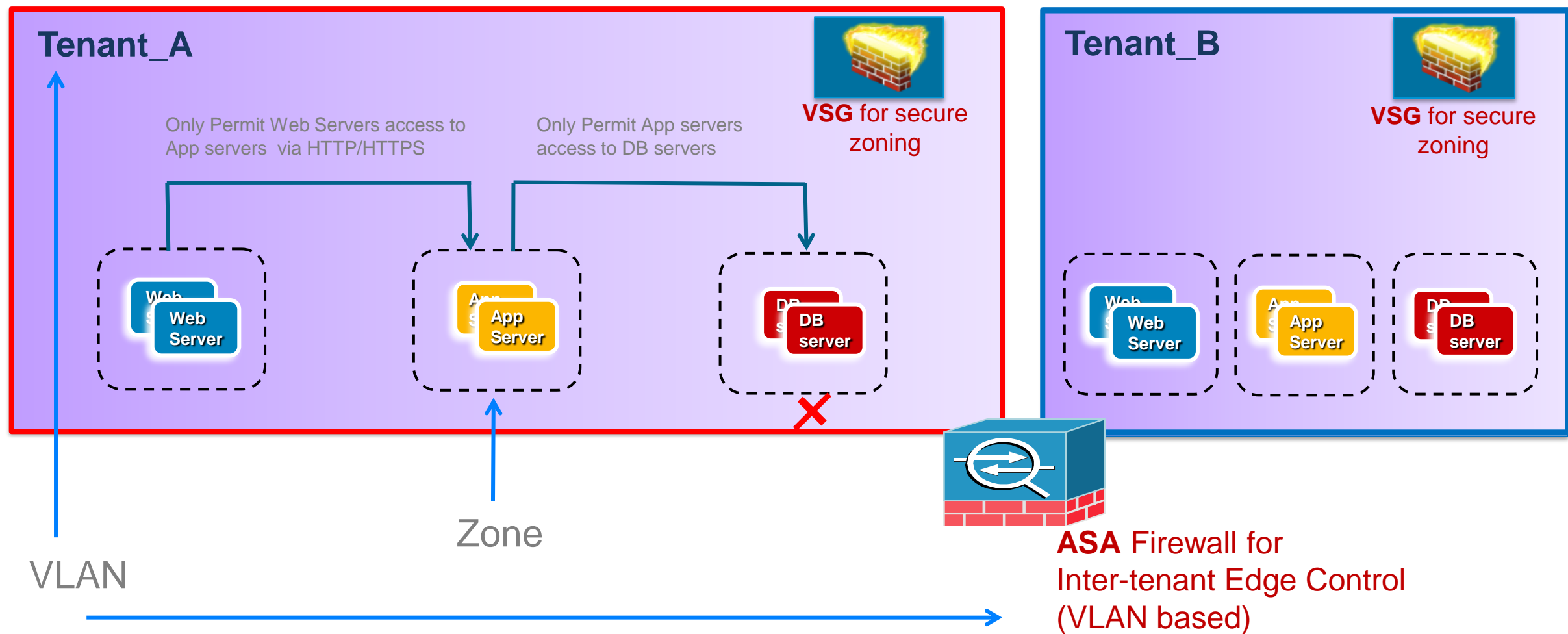
Virtual Security Gateway with vPath Integration



Defense in Depth Security Model

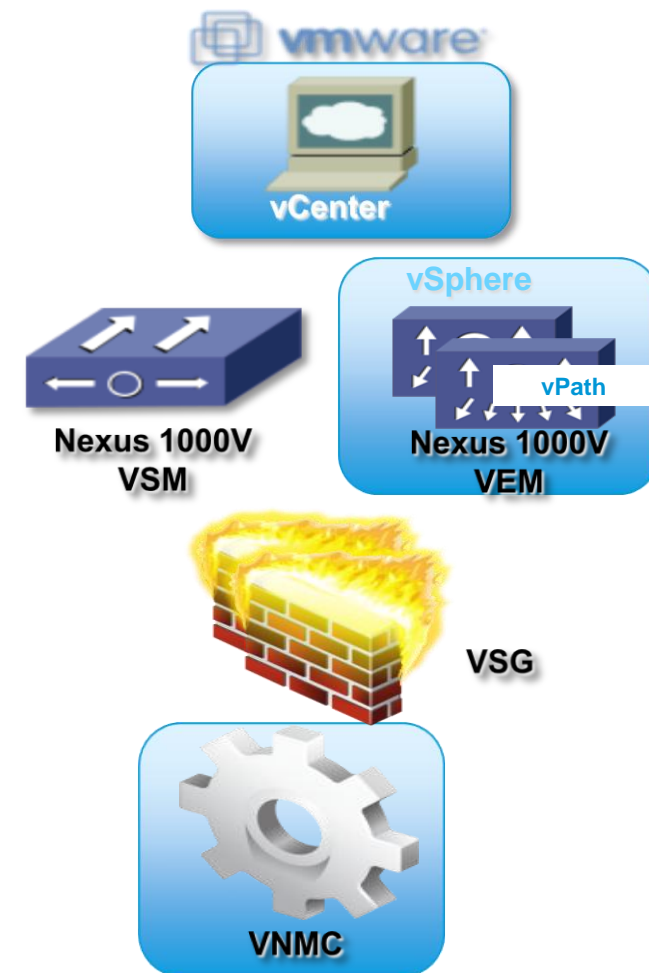


Use Case – Secure Multi-tenancy

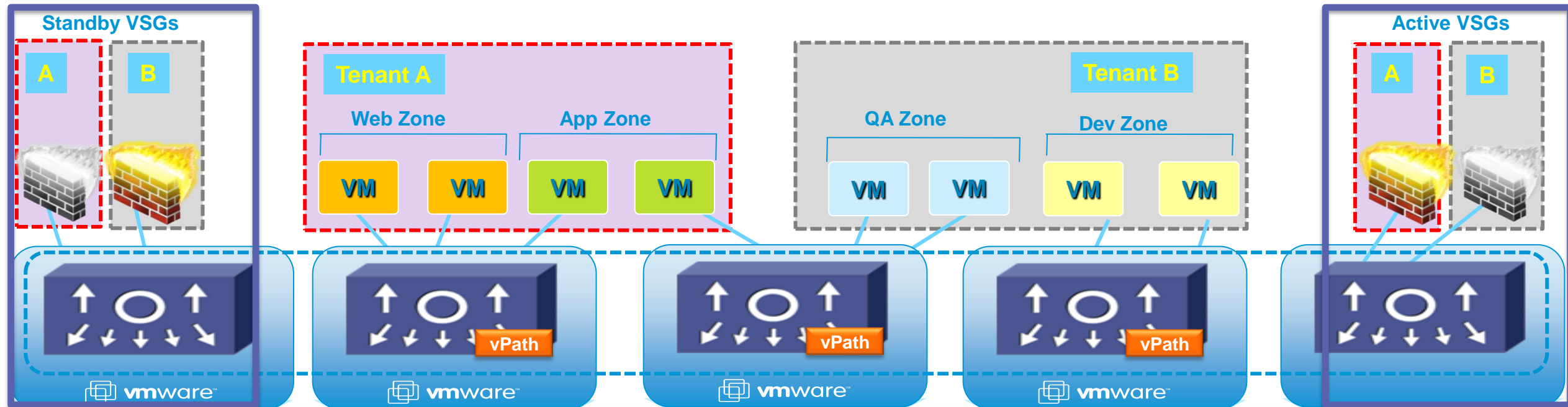


VSG Deployment Requirements

- VMWare vSphere 4.0+ and Virtual Center
- Nexus 1000V Series switch (1.4 or later)
- One (or More) Active VSGs per tenant
- Virtual Network Management Center (VNMC)
- Licensing is based on per protected CPU socket (same as Nexus 1000V)



Deployment VSGs on Dedicated Host



- Dedicated Servers to host VSG Appliances
- Decouple Service from Compute Resources
- Easy to scale out with dedicated hosting of Service

Security Policy Building Block




Rule is analogous to an ACE; Policy is analogous to an ACL

VSG Policy: Rule (ACE) Construct

Rule

☒

☒



Source Condition

Destination Condition

Action

Condition

Attribute Type : Network

Expression

Attribute Name : IP Address

Operator : eq

Attribute Value : 192 . 168 . 1 . 2

☒ drop ☐ permit ☐ reset
☐ log

New

VM Attributes

Instance Name

Guest OS full name

Zone Name

Parent App Name

Port Profile Name

Cluster Name

Hypervisor Name

Network Attributes

IP Address

Network Port

Operator

eq

neq

gt

lt

range

Not-in-range

Prefix

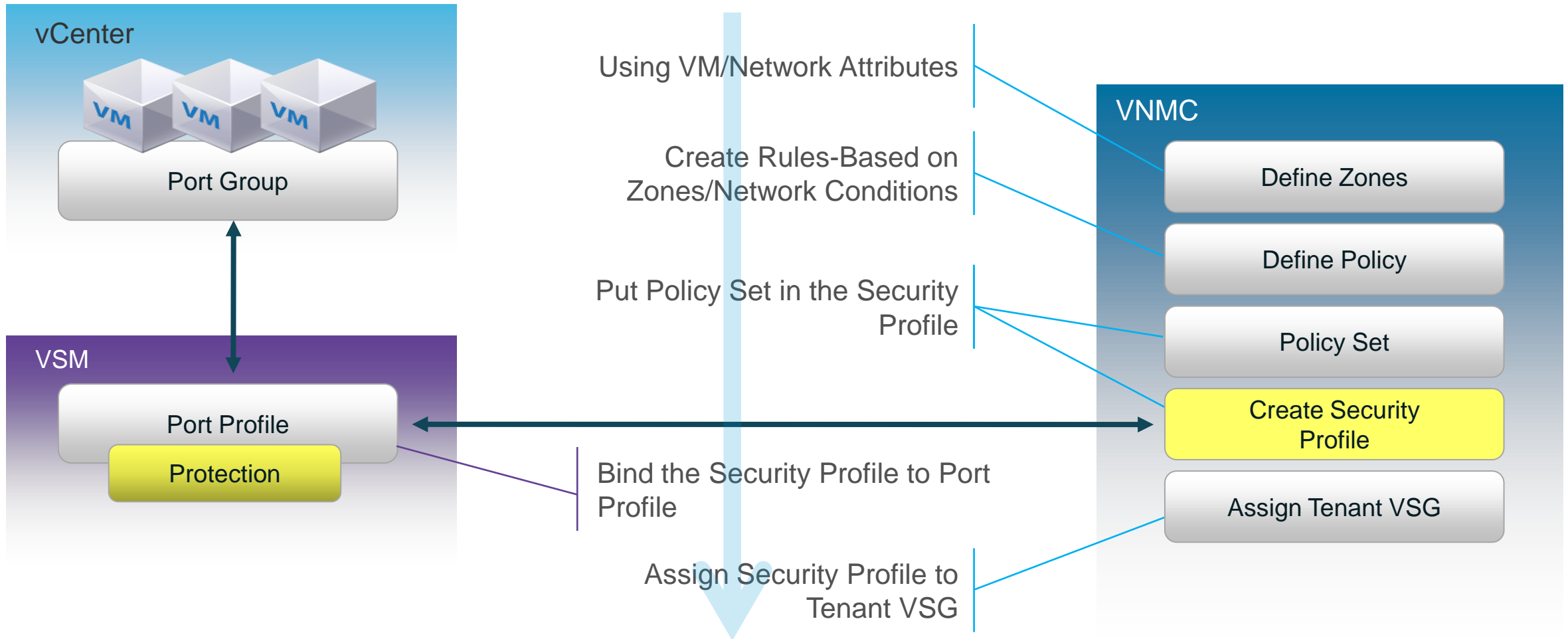
Operator

member

Not-member

Contains

VSG Policy Provisioning Logical Flow



Binding VSG Security Profile with N1kV Port-Profile

Security-Profile “SecureContractors” is attached to Port-Profile “contractor”

The screenshot displays the Virtual Network Management Center (VNC) interface and a terminal window. The VNC interface shows the 'Policy Management' tab with 'Security Policies' selected. Under 'Security Profiles', the 'root' node is expanded, showing 'Security Profiles' and 'Contrator'. The 'Security Profiles' node is highlighted. The 'Security Profiles' table shows a profile named 'SecureContractors'.

The terminal window shows the configuration of the 'SecureContractors' security profile and its binding to the 'contractor' port-profile. The configuration is as follows:

```
org root/Contractor
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractors
no shutdown
state enabled
```

The terminal also shows the command to run the port-profile configuration:

```
N11# sh run port-profile contractor
```

The output of the command is:

```
!Command: show running-config port-profile contractor
!Time: Thu Jan 6 19:24:38 2011

version 4.2(1)SV1(4)
port-profile type vethernet contractor
vmware port-group
switchport access vlan 10
switchport mode access
org root/Contractor
vn-service ip-address 192.168.173.42 vlan 20 security-profile SecureContractors
no shutdown
state enabled
```

A green arrow points from the 'SecureContractors' entry in the VNC table to the 'SecureContractors' entry in the terminal output, indicating the binding of the security profile to the port-profile.

Policy Summary on VSG

```
firewall# show running-config policy

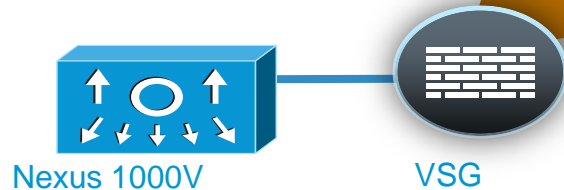
policy default@root
rule default/default-rule@root order 2
policy Deny_Interzone_PolicySet@root/CPOC
rule Deny_Interzone_traffic/Permit_Finance@root/CPOC order 26
rule Deny_Interzone_traffic/Permit_HR@root/CPOC order 51
rule Deny_Interzone_traffic/Deny_HR_to_Finance@root/CPOC order 101
rule Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC order 201
rule Deny_Interzone_traffic/Permit_All@root/CPOC order 301

firewall# show policy-engine stats

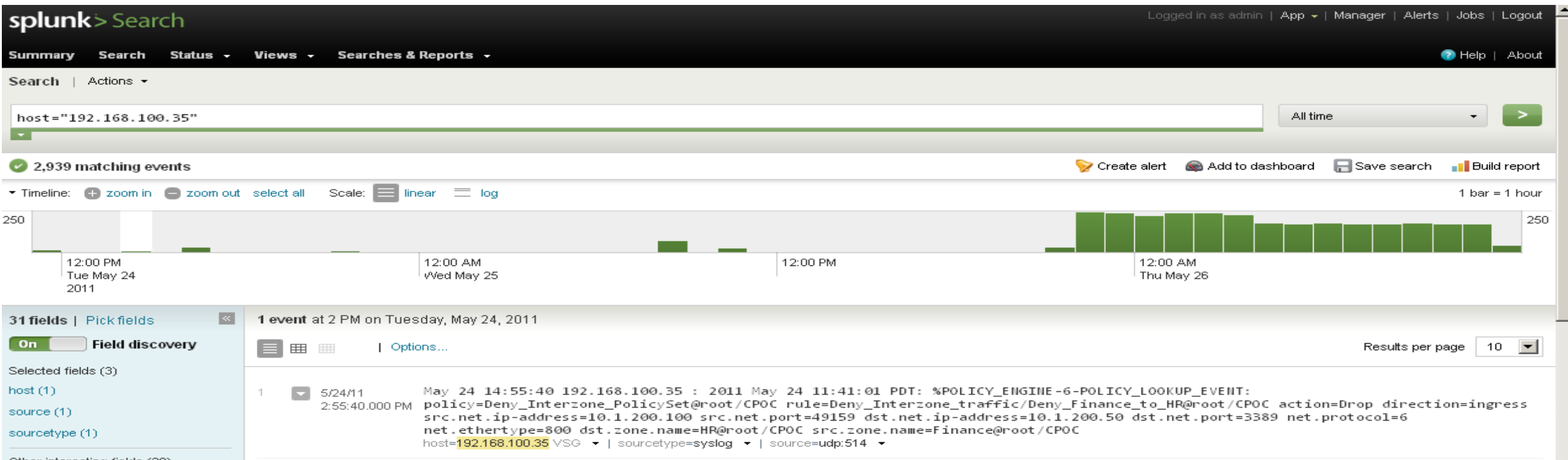
Policy Match Stats:

default@root
default/default-rule@root : 0
NOT_APPLICABLE : 0 <Drop>

Deny_Interzone_PolicySet@root/CPOC
Deny_Interzone_traffic/Permit_Finance@root/CPOC : 7703
Deny_Interzone_traffic/Permit_HR@root/CPOC : 11 <Permit>
Deny_Interzone_traffic/Deny_HR_to_Finance@root/CPOC : 2 <Permit>
Deny_Interzone_traffic/Deny_Finance_to_HR@root/CPOC : 1 <Log, Drop>
Deny_Interzone_traffic/Permit_All@root/CPOC : 2 <Log, Drop>
NOT_APPLICABLE : 7687 <Permit>
NOT_APPLICABLE : 0 <Drop>
```



Syslog from VSG



Use Case

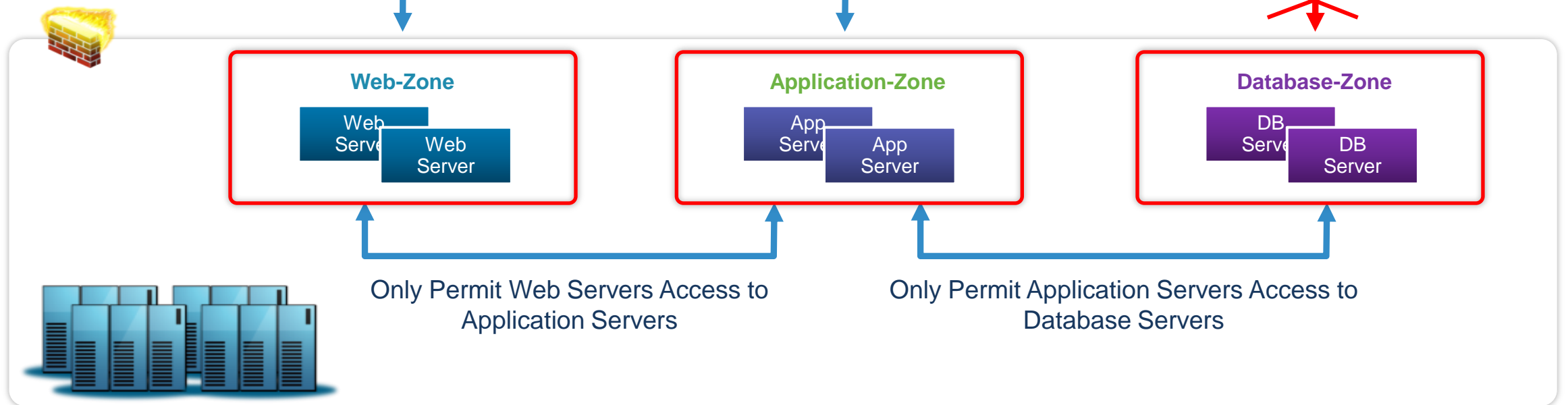
Securing a 3-tier Application Infrastructure



Permit Only Port 80(HTTP) of Web Servers

Permit Only Port 22 (SSH) to Application Servers

Block All External Access to Database Servers



Virtual ASA role in overall architecture



Cisco Virtual Security Products



Virtual Security Gateway

Zone based intra-tenant segmentation of VMs

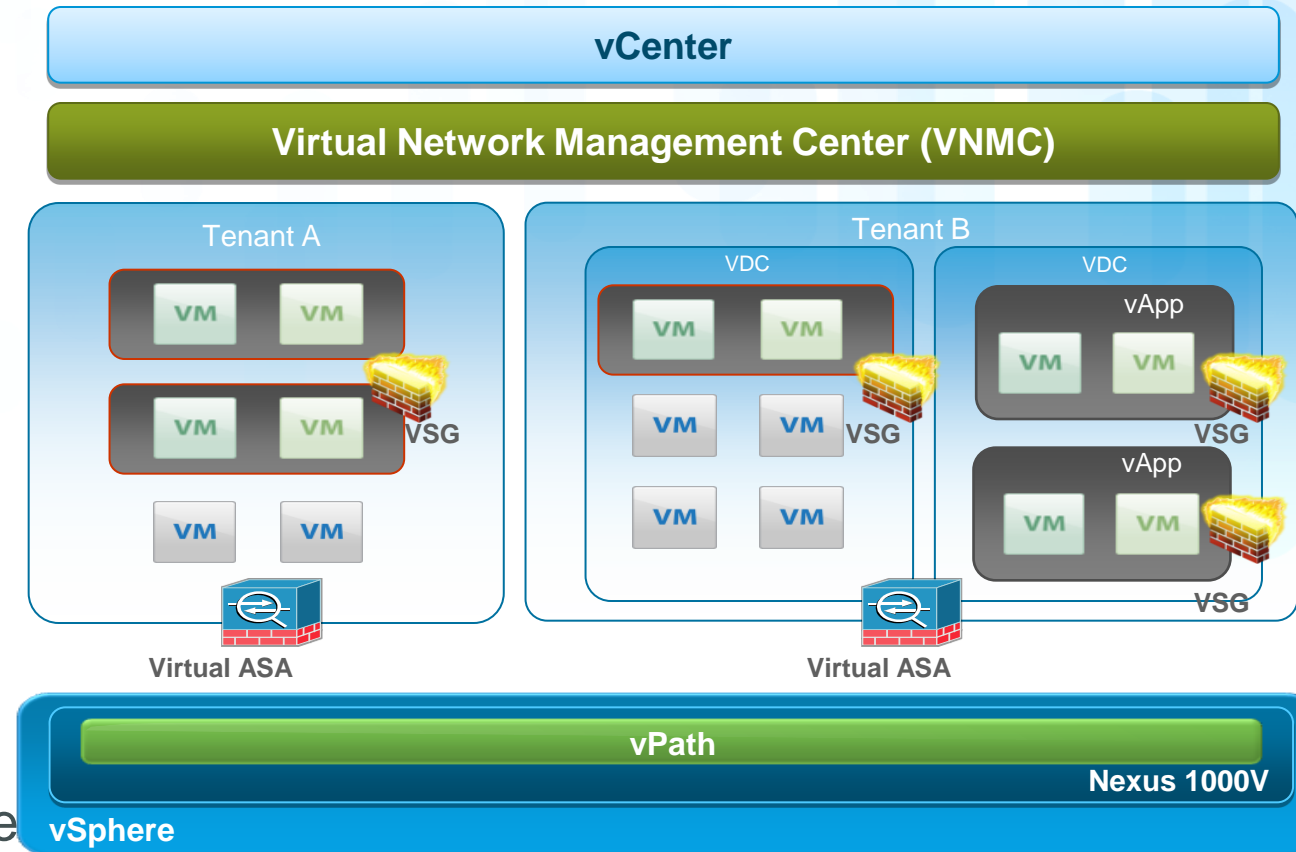


ASA 1000V

External / multi-tenant edge deployment

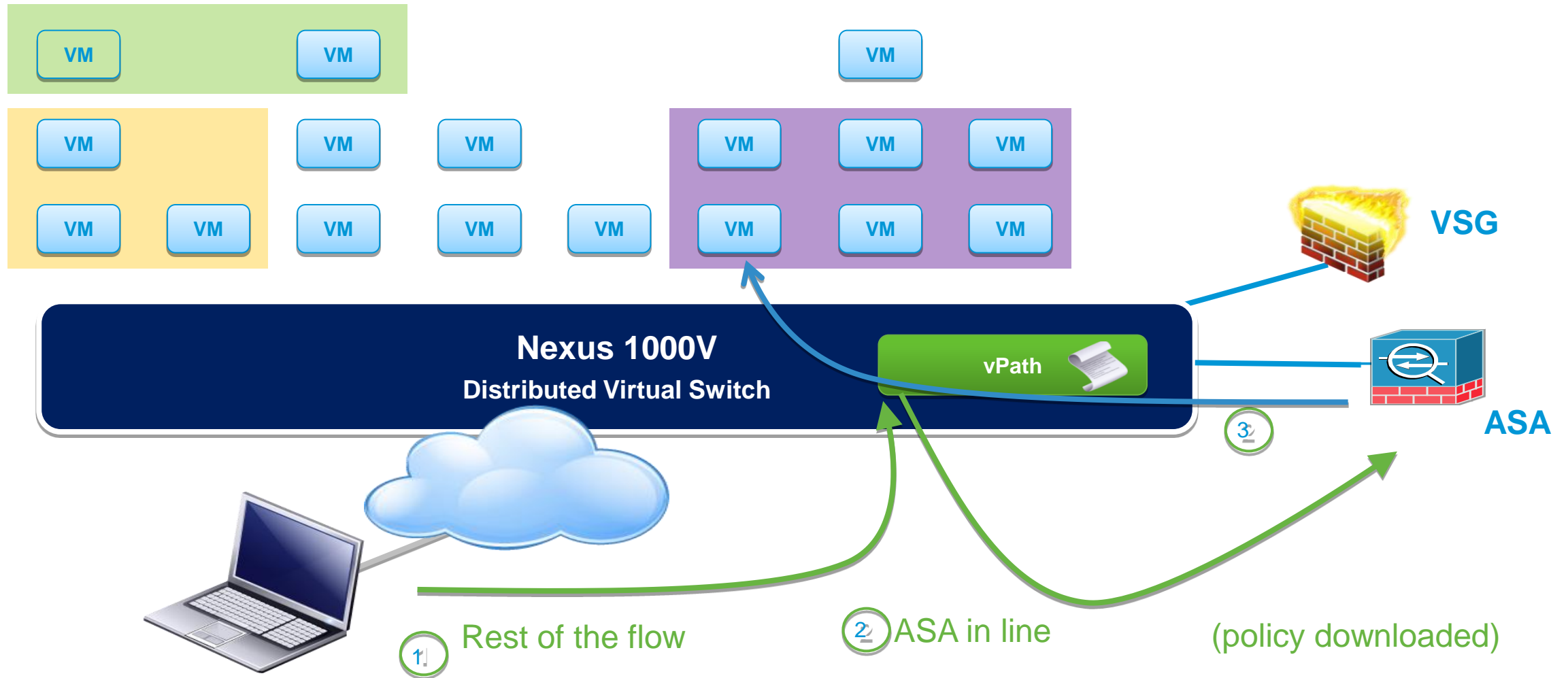
Securing Multi-tenant Cloud

- Proven Cisco Security...Virtualized Physical – virtual consistency
- Collaborative Security Model
VSG for intra-tenant secure zones
Virtual ASA for tenant edge controls
- Seamless Integration
With Nexus 1000V & vPath
- Scales with Cloud Demand
Multi-instance deployment for horizontal scale out deployment



Virtual Security Gateway

ASA Intelligent Traffic Steering with vPath



ASA 1000V 1.0 Features and Capabilities

NAT

IPSec VPN (Site-to-Site)

Default Gateway

DHCP

Static Routing

Stateful Protocol

IP Audit

Role based separation

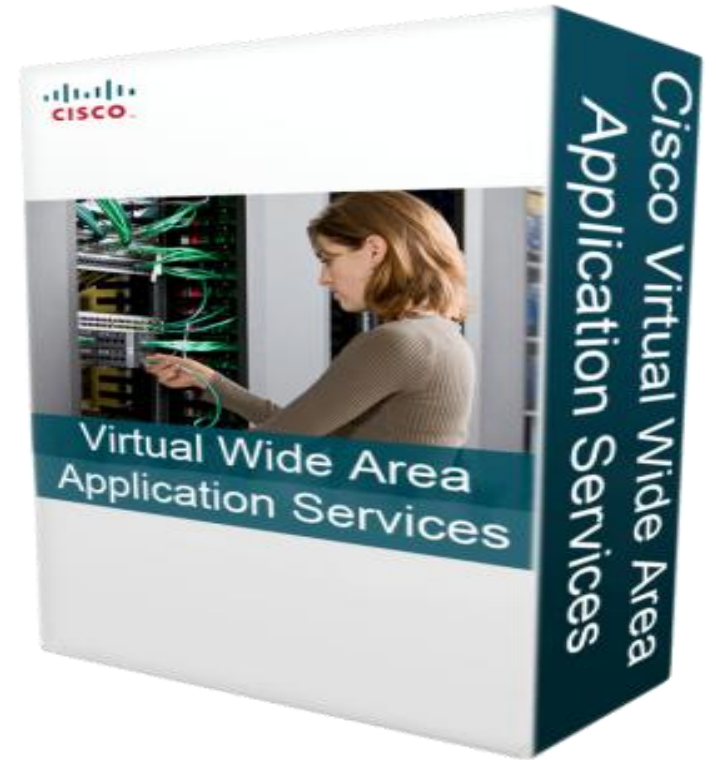
Consistent ASA feature set

Intelligent traffic steering via vPath

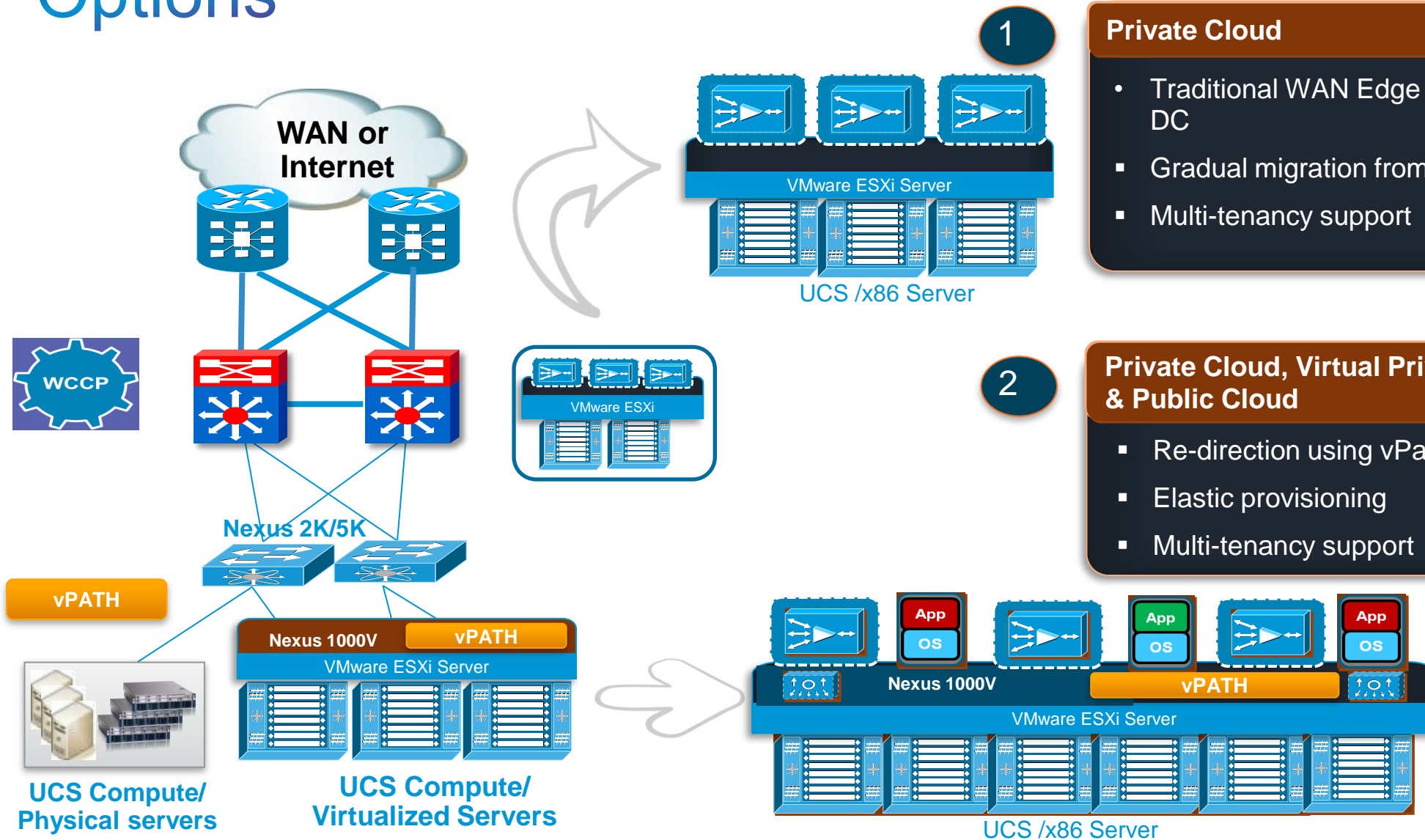
Strategic Partnership with VMWare

Not just an ASA – Part of a solution which benefits from vPath

Virtual WAAS



Cisco vWAAS Provides Flexible Cloud Deployment Options



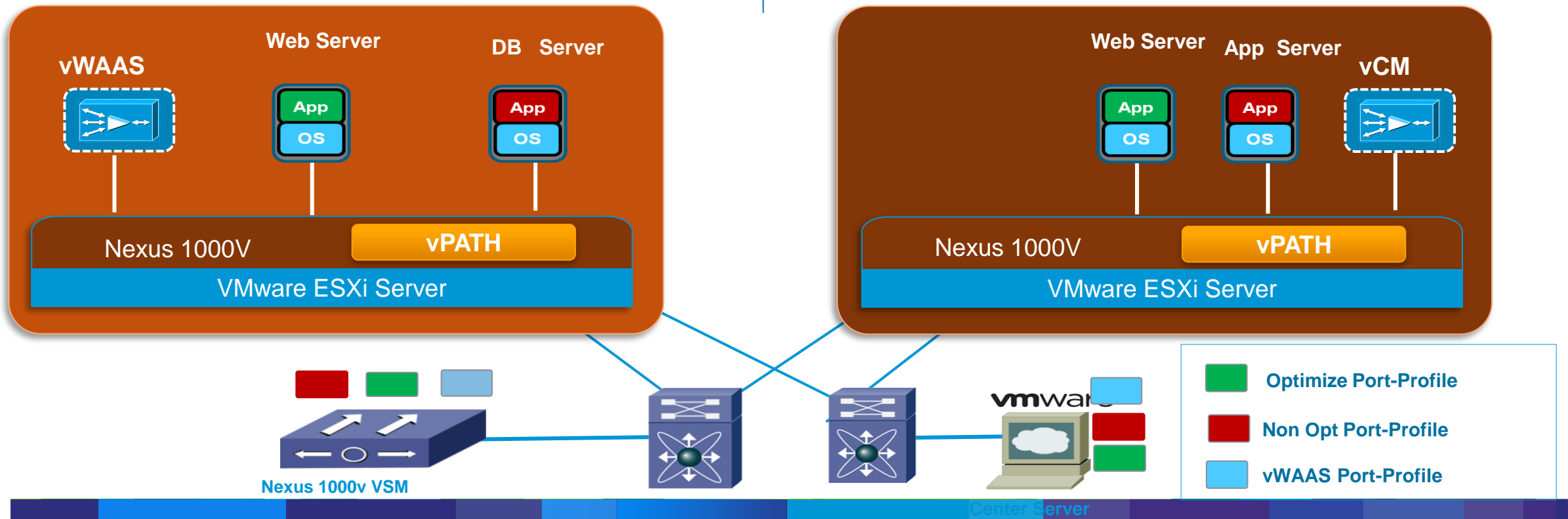
vWAAS – Policy Based configuration in N1000V

Feature

1. Optimization based on the port-profile policy configured in Nexus 1000V
2. Policy gets propagated to vCenter automatically

Benefit

1. Provide on-demand service orchestration in the cloud without network disruption



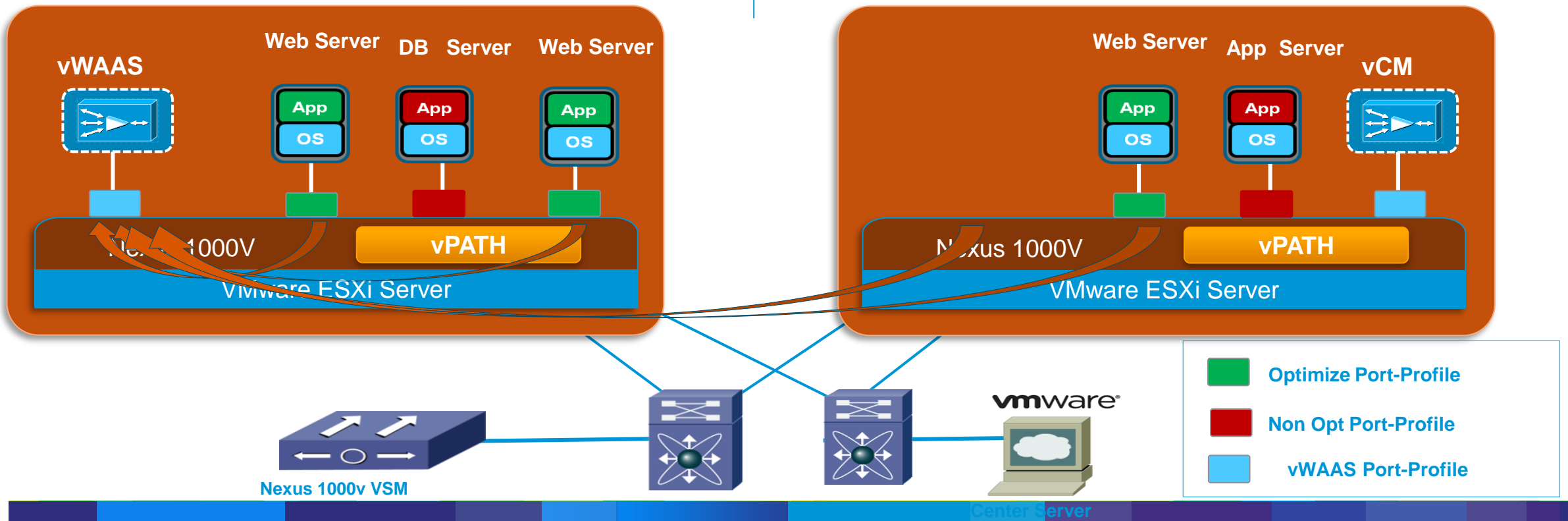
vWAAS – VM mobility awareness

Feature

1. vPATH aware of movement of VM from one host to another.
2. Traffic interception continue to work as-is without any disruption or changes required.

Benefit

1. No disruption in WAN optimization service if VM moves from one host to another.
2. Support VMware resources scheduling (DRS) and provides High availability



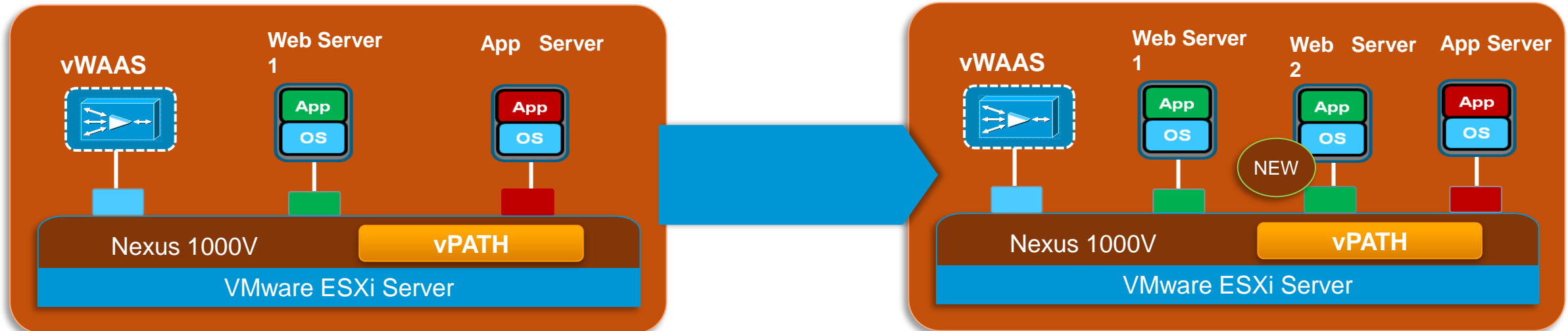
vWAAS – Architected for Elastic Workloads

Feature

1. Automatic application of vWAAS service when a new 'Web Server' VM gets provisioned
2. vWAAS services associated with 'Web server' VMs using Nexus 1000V policies.

Benefit

1. Elastic vWAAS deployment
2. Scale-out Virtual Web Server farm by provisioning additional VMs while applying WAN optimization



Resume

- Shift in Virtual Network Services strategy
- VXLAN extends L2 boundaries and extend VLAN IDs for vCD
- vPath traffic interception without topology change
- Nexus 1000V is foundation for virtual services
- Virtual Security Gateway zone based firewall between VMs
- Virtual ASA is edge firewall for traffic entering/leaving tenants
- Virtual WAAS easy traffic optimization in virtual environment

Upcoming Public Webcasts, Spring 2012

Open to Customers and Partners

Date	Technical Track Topics	Webinar
2/14/12	Virtual Security Gateway (VSG) v1.3 Technical Deep Dive	Register
2/22/12	Nexus 1000V v1.5 Technical Deep Dive	Register
2/29/12	Nexus 1010-X v1.4 Technical Deep Dive	Register
3/7/12	vWAAS and Nexus 1000V Technical Deep Dive	Register
3/14/12	FlexPod & Nexus 1000V/1010	Register
3/21/12	QoS for multimedia traffic in the Virtualized DC (w/ Nexus 1000V)	Register
3/28/12	Vblock & Nexus 1000V / VSG / vWAAS	Register
4/4/12	vCloud Director, Nexus 1000V, and VXLAN Technical Deep Dive	Register
4/11/12	Cisco's CloudLab Deep Dive: Hands-on labs for N1KV, VSG & VXLAN	Register

Webinar Link: www.cisco.com/go/1000vcommunity

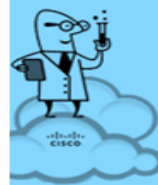
Cisco Cloud Lab

Hands On Training & Demos

- Hands on labs available for Nexus 1000V and VSG in Cloud Lab

<https://cloudlab.cisco.com>

- Open to all Cisco employees
- Customers/Partners require sponsorship from account team for access via CCO LoginID
- Extended duration lab licenses for 1000V and VSG are available upon request



Welcome to Cisco CloudLab

Please select one of the available labs, by clicking on its name. Hover over the lab name content.

Available labs:

- Cisco Nexus 1000V - Basic Introduction (N1K-000111)
- Cisco Nexus 1000V - Installation (N1K-000211)
- Cisco Nexus 1000V - Upgrade to 1.4 (N1K-000310)
- Cisco Virtual Security Gateway (VSG) - Introduction (VSG-000110)
- Cisco Nexus 7000 - Introduction to NX-OS (N7K-000110)
- Cisco Overlay Transport Virtualization (OTV) (N7K-000210)
- Demo: Cisco Nexus 1000V (Pre-Configured) (N1K-100111)
- Demo: Cisco Virtual Security Gateway (VSG)(Pre-Configured) (VSG-100110)

Thank you.

